Translation of DE 195 35 019 A1

Description

The present invention relates to a magnetic storage medium, especially a magnetic card having a magnetic strip, on which raw data having a particular information content are stored in encrypted form.

The encryption of raw data on magnetic storage media is necessary in order to make it difficult or impossible for unauthorised third parties to gain access to the raw data. There are various possibilities for illegally reproducing magnetic cards.

For example, the data on one magnetic card can be copied onto a second card. For that purpose, a relatively simple apparatus is sufficient, consisting of a reading head and a writing head connected thereto by way of an electronic amplifier. Whilst the reading head is passed over the magnetic strip on the first magnetic card, the writing head simultaneously stores the read data onto the magnetic strip of the second magnetic card.

This illegal copying of magnetic cards is especially widespread in the case of credit cards. Using those forged credit cards it is possible to cause a great deal of damage because they are used without additional security precautions (e.g. secret number, PIN) and can be used for relatively large sums of money.

Magnetic cards are also used for controlling access to transportation (travel tickets), ski lifts (ski passes) or events (entry tickets).

Such magnetic cards for travel tickets, ski passes or entry tickets consist of a flexible carrier material of plastics or paper to which there is applied a magnetic strip, which contains the raw data carrying the information (e.g. location and date of issue, duration of validity). Increasingly, such magnetic cards are also being reproduced by being cut along the magnetic strip in the longitudinal direction. These halved magnetic strips are stuck onto substrates of the same size as the original magnetic cards. The coercivity of the halved magnetic strip is sufficient in most cases still to be read by the magnetic card reader.

From EP 0 313 063 A2 there is known an encryption method wherein a pattern of a magnetic material having a coercivity of less than 30 oersted is applied to the magnetic strip. The position and local extent of the magnetic pattern are known. That knowledge is taken into account when de-encrypting the data that have been stored on the magnetic strip and encrypted by the magnetic pattern. The information necessary for de-encryption of the data must accordingly be available in the magnetic card reading devices. In order to be able to ensure the compatibility of the individual magnetic cards with the magnetic card reading devices, the individual magnetic cards must be encrypted with the same magnetic pattern.

It is accordingly still possible to copy the contents of such magnetic cards, using a simple read/write device, from an encrypted magnetic card onto another likewise encrypted card. A fundamental possibility of forging magnetic cards is not removed by that encryption method.

The present invention is based on the problem of so developing a magnetic storage medium of the kind mentioned at the beginning that copying or forgery is made substantially more difficult or even impossible.

For solving the problem, the invention proposes, starting from the magnetic storage medium of the kind mentioned at the beginning, that a freely selectable pattern of a magnetic material having a coercivity that differs from the coercivity of the magnetic strip is applied to the magnetic strip.

The invention makes it possible to apply an individual pattern to virtually any magnetic card. As a result of the application of such a magnetic pattern to the magnetic strip, the coercivity of the magnetic strip is no longer homogeneous but has non-homogeneous properties.

The different patterns on the magnetic cards obviate the need for the information required for de-encryption to be present in the magnetic card reading device, because the de-encryption information varies from one magnetic card to another. In the case of the magnetic card according to the invention, the information for de-encryption can be extracted from the data contained on the magnetic strip, for each magnetic card separately.

In the case of the magnetic cards according to the invention this is performed as follows: The raw data are generally placed on the magnetic card by means of periodic flux changes of the magnetic field on the magnetic strip. In the case of magnetic cards having unencrypted data and conventional magnetic strips having a homogeneous magnetic material of constant coercivity, the amplitudes of the magnetic flux are of a constant magnitude. In the case of magnetic cards with encrypted data and magnetic strips to which, in accordance with the invention, a pattern of a magnetic material of differing coercivity has been applied, the amplitudes of the magnetic flux vary in dependence upon the differing coercivity of the magnetic strip. On the basis of the varying amplitudes of the magnetic flux, it is possible, in dependence upon the periodic flux changes, to determine the absolute position and extent of the pattern on the magnetic strip and the coercivity of the magnetic strip in question. Using that information, the raw data can be extracted from the voltage signal induced in the reading head of the magnetic card reading device.

Magnetic cards encrypted with individual patterns in that manner can consequently be read and de-encrypted by a single type of magnetic card reading device, without the latter knowing the pattern beforehand.

After the raw data have been read and de-encrypted, they are manipulated. For example, the duration of the validity of the magnetic card may be extended or a particular sum may be deducted from the credit balance on the card. The manipulated raw data are then written back to the magnetic card. In the process, the information used for de-encrypting the data controls the magnitude of the writing current of the writing head. In regions of high coercivity in the magnetic strip, a higher writing current must be used than in the regions of low coercivity. As a result it is possible to write only to those magnetic cards whose de-encryption information has been ascertained previously.

As a result, the manipulated raw data are stored in encrypted form on the magnetic card in dependence upon the position and extent of the pattern and the coercivity of the magnetic strip.

The precondition for writing to such magnetic cards is a read/write head in a magnetic card reading device, wherein the writing current can be controlled. In addition, magnetic cards having such a freely selectable pattern must be provided with data before the first

reading procedure, preferably in the factory. In that process, it is not the content of the data that is important but rather the fact that they are placed on the magnetic strip by means of periodic flux changes. These flux changes are required for locating the position and extent of the magnetic pattern on the magnetic strip and for determining the coercivity of the magnetic strip. The de-encryption information for the magnetic card in question is extracted from those details.

Copying the data of magnetic cards by means of a simple read/write device is made impossible by the encrypted magnetic card according to the invention. The differing coercivity of the pattern and magnetic strip and the fact that the pattern is different on almost every magnetic card means that the voltage induced in the reading head from the magnetic strip of a first magnetic card is not proportional to the writing current of the writing head for the magnetic strip of a second magnetic card. The data read from a first magnetic card are therefore incorrectly transferred to a second card. The consequence is that the copied magnetic card contains entirely incorrect data or is entirely unreadable.

Copying the magnetic cards by cutting down the centre of the magnetic strip in the longitudinal direction is also prevented by the data encryption method according to the invention. The application of a freely selectable pattern also makes it possible for patterns to be applied asymmetrically relative to the longitudinal axis of the magnetic strip. This means that dividing the magnetic strip longitudinally results in two magnetic strips having different magnetic patterns. It will be highly probable that the two halved magnetic strips will be unreadable with the data present thereon. This occurs because the data were originally stored using the de-encryption information obtained from the entire magnetic strip. When a halved magnetic strip is read, different de-encryption information is obtained as a result of the different position and extent of the magnetic pattern, which cannot be used to de-encrypt the data originally placed on the magnetic card.

In a preferred embodiment of the invention, the coercivity of the magnetic material of the pattern is several times the coercivity of the magnetic strip.

There is a pronounced difference between the coercivity of the magnetic material of the pattern and the coercivity of the material of the magnetic strip. This makes it possible for the pattern to be clearly differentiated from the magnetic strip. Problems that may possibly occur in locating the magnetic pattern because of an insufficient difference

between the coercivity of the pattern and that of the magnetic strip are accordingly avoided. The number of unreadable or incorrectly encrypted magnetic cards is reduced to a minimum.

In further embodiments of the invention, the freely selectable pattern has a random or ordered shape.

The pattern is applied to the magnetic strip by various magnetic materials. For example, magnetic dispersions, magnetic filings, or foils of magnetic materials can be envisaged. The shape of the pattern may be subjected to random chance or may be ordered. Such ordered forms of the magnetic pattern are, for example, geometric shapes or combinations of letters.

In both forms of the magnetic pattern it must, however, be ensured that the magnetic strip and the magnetic pattern have a uniform colour in order to prevent the position and extent of the magnetic pattern being discernible to the eye from the outside and information for de-encryption being obtained therefrom. It is, however, conceivable, for example for advertising purposes, to apply, in addition to the magnetic pattern within the colour of the magnetic strip, a further coloured pattern in the form of a company logo or a letter combination in a colour that differs from the colour of the magnetic strip.

The invention will be explained hereinbelow in greater detail with reference to a drawing and a flow diagram, wherein:

Fig. 1 shows an embodiment of the magnetic card encrypted in accordance with the invention;

Fig. 2 is a flow diagram for the de-encryption and re-encryption of data on a magnetic card encrypted in accordance with the invention.

In Fig. 1, the reference numeral 1 denotes a magnetic card. A magnetic strip 3 is applied to a carrier material 2. The carrier material 2 consists of, for example, paper or plastics. For encryption of the data stored on the magnetic strip, the latter is provided with a magnetic pattern 4, 5. The pattern 4, 5 consists of, for example, magnetic filings, a magnetic dispersion, or foil of magnetic materials and is applied to the magnetic strip 4, 5. The magnetic pattern 4, 5 can have freely selectable shapes. The pattern 4

has a random shape, whereas the pattern 5 has an ordered shape, for example a letter combination.

Fig. 2 is a flow diagram illustrating in greater detail the various steps in de-encrypting and encrypting data on a magnetic strip of a magnetic card encrypted in accordance with the invention. First of all, the position and extent of the magnetic pattern on the magnetic strip and the coercivity of the magnetic strip are determined in dependence upon the flux change. The de-encryption information is extracted from those details. Using that de-encryption information, the raw data are determined from the encrypted data read. The raw data are then manipulated on the basis of external events; for example, the duration of validity of the magnetic card is extended. The manipulated raw data must then be written back to the card. Using the de-encryption information, the raw data are re-encrypted and, by appropriately controlling the writing current of a writing head, are stored on the magnetic strip of the magnetic card.

Nummer: DE 195 35 0.
Int. Cl.[6]: G 11 B 5/70
Offenlegungstag: 27. März 1997

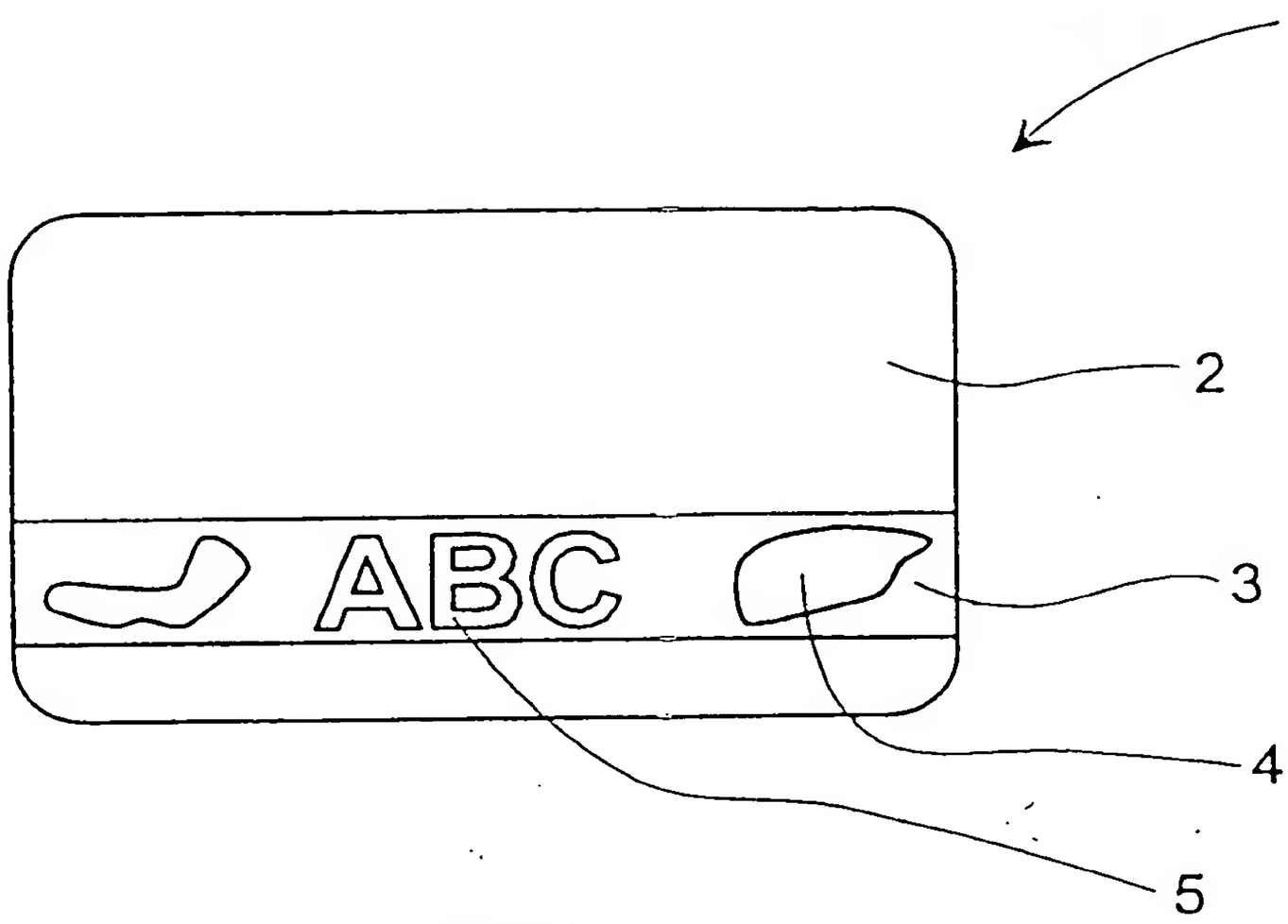


Fig. 1

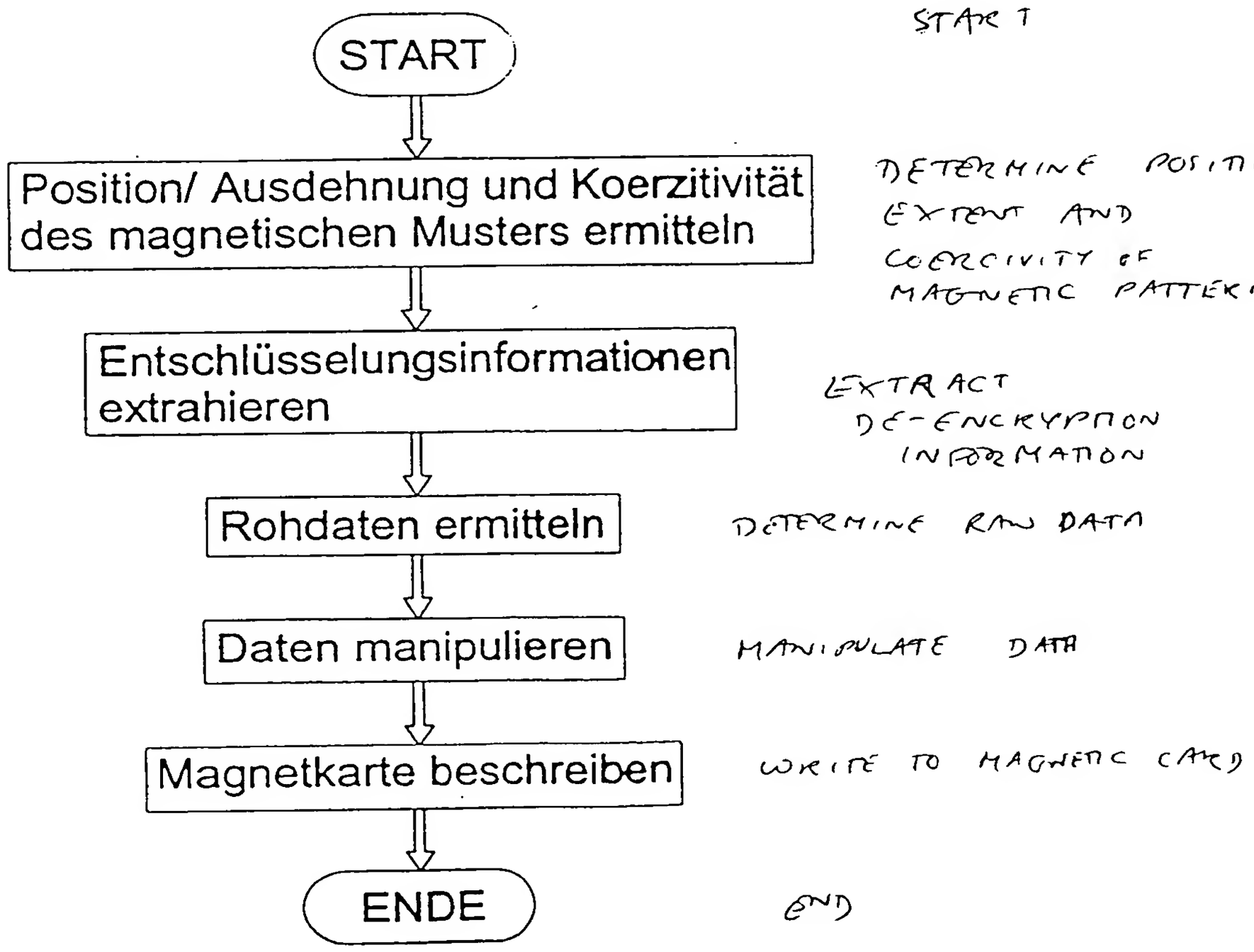


Fig. 2

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(10) Offenlegungsschrift DE 195 35 019 A 1

(51) Int. Cl.[6]:
G 11 B 5/70
G 11 B 23/28
// G07C 9/00,G07F 7/08

(21) Aktenzeichen: 195 35 019.7
(22) Anmeldetag: 21. 9. 95
(43) Offenlegungstag: 27. 3. 97

(71) Anmelder:
CardTec Entwicklungs- und Vertriebsgesellschaft für elektronische Kartensysteme mbH, 44795 Bochum, DE

(74) Vertreter:
Schneiders · Behrendt · Finkener · Ernesti, Rechtsanwälte · Patentanwälte, European Patent Attorneys, 44787 Bochum

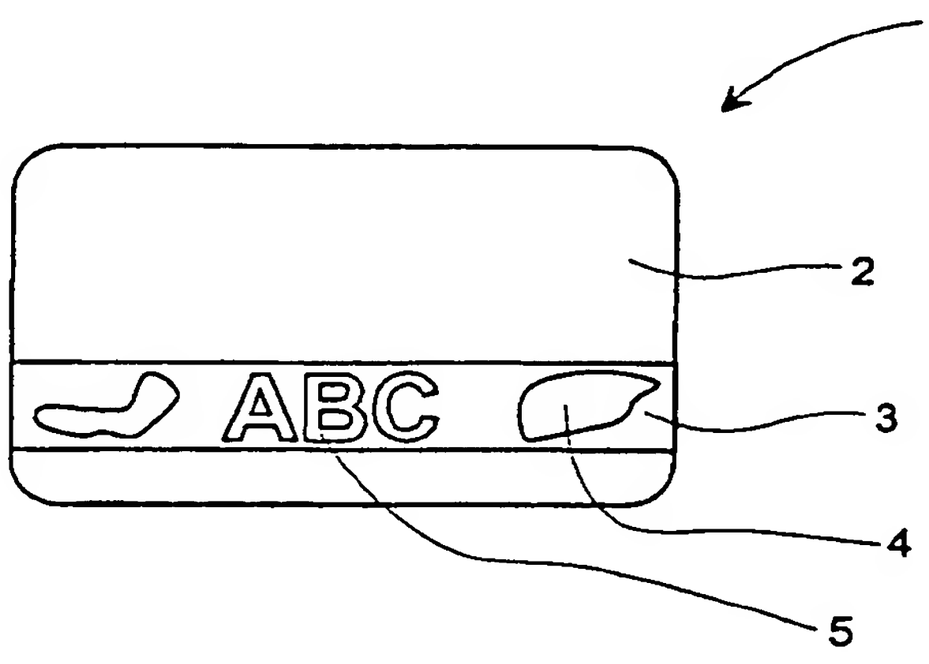
(72) Erfinder:
Künstler, Rainer, 44795 Bochum, DE

(56) Entgegenhaltungen:
DE 36 17 319 C2
DE 37 05 006 A1

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Magnetisches Speichermedium mit verschlüsselten Rohdaten

(57) Die vorliegende Erfindung betrifft ein magnetisches Speichermedium, insbesondere eine Magnetkarte (1) mit einem Magnetstreifen (3), auf dem Rohdaten mit einem bestimmten Informationsgehalt in verschlüsselter Form abgespeichert sind. Um das Kopieren oder Fälschen solcher magnetischer Speichermedien wesentlich zu erschweren oder sogar unmöglich zu machen, schlägt die Erfindung vor, auf dem Magnetstreifen (3) ein beliebiges Muster (4, 5) aus einem magnetischen Material mit einer von der Koerzitivität des Magnetstreifens (3) abweichenden Koerzitivität aufzubringen. Vorteilhaft weist die Koerzitivität des magnetischen Materials des Musters (4, 5) ein Mehrfaches der Koerzitivität des Magnetstreifens (3) auf. Aus der Position und Ausdehnung des magnetischen Musters (4, 5) auf dem Magnetstreifen (3) und der Koerzitivität des Magnetstreifens (3) werden Entschlüsselungsinformationen ermittelt, mit deren Hilfe aus den verschlüsselten Daten die auf der Magnetkarte (1) gespeicherten Rohdaten extrahiert.



DE 195 35 019 A 1

Beschreibung

Die vorliegende Erfindung betrifft ein magnetisches Speichermedium, insbesondere eine Magnetkarte mit einem Magnetstreifen, auf dem Rohdaten mit einem bestimmten Informationsgehalt in verschlüsselter Form abgespeichert sind.

Das Verschlüsseln von Rohdaten auf magnetischen Speichermedien ist notwendig, um unberechtigten Dritten den Zugang zu diesen Rohdaten zu erschweren oder unmöglich zu machen. Es gibt verschiedene Möglichkeiten, Magnetkarten illegal zu vervielfältigen.

Man kann beispielsweise die Daten einer Magnetkarte auf eine zweite kopieren. Dazu genügt eine relativ einfache Vorrichtung, bestehend aus einem Lesekopf und einem mit diesem über einen elektronischen Verstärker verbundenen Schreibkopf. Während der Lesekopf über den Magnetstreifen der einen Magnetkarte gleitet, speichert der Schreibkopf diese eingelesenen Daten gleichzeitig auf dem Magnetstreifen der zweiten Magnetkarte.

Dieses illegale Kopieren von Magnetkarten ist besonders bei Kreditkarten verbreitet. Mit diesen gefälschten Kreditkarten kann ein hoher Schaden angerichtet werden, da sie ohne zusätzliche Sicherheitsvorkehrungen (z. B. Geheimnummer, PIN) eingesetzt werden und sic für relativ große Geldbeträge einsetzbar sind.

Magnetkarten werden auch als Zugangskontrolle für Verkehrsmittel (Fahrscheine), Skilifte (Skipässe) oder Veranstaltungen (Eintrittskarten) verwendet.

Diese Magnetkarten für Fahrkarten, Skipässe oder Eintrittskarten bestehen aus einem flexiblen Trägermaterial aus Kunststoff oder Papier, auf welchem der Magnetstreifen aufgebracht ist, der die Rohdaten mit den Informationen (z. B. Ausstellungsort, Ausstellungsdatum, Gültigkeitsdauer) enthält. In zunehmendem Maße werden auch solche Magnetkarten illegal vervielfältigt, indem sie mittig entlang des Magnetstreifens in Längsrichtung durchschnitten werden. Diese halben Magnetstreifen werden auf Unterlagen geklebt, die die Größe der ursprünglichen Magnetkarten haben. Die Koerzitivität des halben Magnetstreifens reicht in den meisten Fällen aus, um vom Magnetkartenleser noch eingelesen werden zu können.

Aus der EP 0 313 063 A2 ist ein Verschlüsselungsverfahren bekannt, bei dem ein Muster aus einem magnetischen Material mit einer Koerzitivität, die kleiner als 30 Oersted ist, auf den Magnetstreifen aufgebracht ist. Die Position und die örtliche Ausdehnung des magnetischen Musters auf dem Magnetstreifen sind bekannt. Dieses Wissen wird beim Entschlüsseln der durch das magnetische Muster verschlüsselten, auf dem Magnetstreifen abgelegten Daten berücksichtigt. Die zum Entschlüsseln der Daten notwendigen Informationen müssen also in den Magnetkarten-Lesegeräten vorhanden sein. Um die Kompatibilität der einzelnen Magnetkarten mit den Magnetkarten-Lesegeräten gewährleisten zu können, müssen die einzelnen Magnetkarten mit dem gleichen magnetischen Muster verschlüsselt werden.

Es ist damit weiterhin möglich, den Inhalt solcher Magnetkarten mit einem einfachen Lese-/Schreibgerät von einer verschlüsselten Magnetkarte auf eine andere, ebenso verschlüsselte zu kopieren. Eine wesentliche Möglichkeit, Magnetkarten zu fälschen, wird durch dieses Verschlüsselungsverfahren nicht beseitigt.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein magnetisches Speichermedium der eingangs genannten Art dahingehend weiterzubilden, daß das Kopieren oder Fälschen wesentlich erschwert oder sogar unmöglich gemacht wird.

Zur Lösung dieser Aufgabe schlägt die Erfindung ausgehend von dem magnetischen Speichermedium der eingangs genannten Art vor, daß auf dem Magnetstreifen ein beliebiges Muster aus einem magnetischen Material mit einer von der Koerzitivität des Magnetstreifens abweichenden Koerzitivität aufgebracht ist.

Die Erfindung macht es möglich, auf nahezu jede Magnetkarte ein individuelles Muster aufzubringen. Durch das Aufbringen eines solchen magnetischen Musters auf den Magnetstreifen ist die Koerzitivität des Magnetstreifens nicht mehr homogen, sondern weist inhomogene Eigenschaften auf.

Die unterschiedlichen Muster auf den Magnetkarten machen es überflüssig, daß die zur Entschlüsselung nötigen Informationen in dem Magnetkarten-Lesegerät vorhanden sind, da die Entschlüsselungsinformationen von Magnetkarte zu Magnetkarte variieren. Bei der Magnetkarte gemäß der Erfindung können die Informationen für die Entschlüsselung aus den auf dem Magnetstreifen enthaltenen Daten für jede Magnetkarte gesondert extrahiert werden.

Dies geschieht bei der erfindungsgemäßen Magnetkarten folgendermaßen: Die Rohdaten werden auf der Magnetkarte im allgemeinen mittels periodischer Flußwechsel des Magnetfeldes auf dem Magnetstreifen abgelegt. Bei Magnetkarten mit unverschlüsselten Daten und herkömmliche Magnetstreifen aus einem homogenen magnetischen Material konstanter Koerzitivität weisen die Amplituden des magnetischen Flusses eine konstante Größe auf. Bei Magnetkarten mit verschlüsselten Daten und Magnetstreifen, auf denen gemäß der Erfindung ein Muster aus einem magnetischen Material abweichender Koerzitivität aufgebracht ist, variieren die Amplituden des magnetischen Flusses abhängig von der unterschiedlichen Koerzitivität des Magnetstreifens. Aufgrund der unterschiedlichen Amplituden des magnetischen Flusses kann man abhängig von den periodischen Flußwechseln die absolute Position und Ausdehnung des Musters auf dem Magnetstreifen und die jeweilige Koerzitivität des Magnetstreifens ermitteln. Mit Hilfe dieser Informationen können aus dem im Lesekopf des Magnetkarten-Lesegerätes induzierten Spannungssignal die Rohdaten extrahiert werden.

Derart mit individuellen Mustern verschlüsselte Magnetkarten können folglich von einem einzigen Magnetkarten-Lesegerättyp eingelesen und entschlüsselt werden, ohne daß dieser vorher das Muster kennt.

Nach dem Einlesen und Entschlüsseln der Rohdaten werden diese manipuliert. Es kann beispielsweise die Verlängerung der Gültigkeitsdauer der Magnetkarte oder das Abbuchen eines bestimmten Betrages von einem Kartenguthaben durchgeführt werden. Die manipulierten Rohdaten werden dann wieder auf die Magnetkarte zurückgeschrieben. Dabei steuern die Informationen, die zum Entschlüsseln der Daten benutzt wurden, die Stärke des Schreibstromes des Schreibkopfes. In den Bereichen hoher Koerzitivität des Magnetstreifens muß dabei mit einem höheren Schreibstrom gearbeitet werden als in den Bereichen niedriger Koerzitivität. Damit können nur solche Magnetkarten beschrieben werden, deren Entschlüsselungsinformation vorher auch ermittelt worden sind.

Damit sind die manipulierten Rohdaten abhängig von Position und Ausdehnung des Musters und der Koerzitivität des Magnetstreifens auf der Magnetkarte verschlüsselt gespeichert.

Die Voraussetzung für ein Beschreiben derartiger Magnetkarten ist ein Lese-/Schreibkopf in einem Magnetkarten-Lesegerät, dessen Schreibstrom steuerbar ist. Außerdem müssen Magnetkarten, die mit einem solchen beliebigen Muster versehen sind, vor dem ersten Lesevorgang, vorzugsweise bereits ab Werk, mit Daten beschrieben sein. Dabei ist nicht der Inhalt dieser Daten wichtig, sondern vielmehr die Tatsache, daß sie auf den Magnetstreifen mittels periodischer Flußwechsel abgelegt sind. Diese Flußwechsel werden zum Lokalisieren der Position und Ausdehnung des magnetischen Musters auf dem Magnetstreifen und zur Bestimmung der Koerzitivität des Magnetstreifens benötigt. Aus diesen Angaben werden die Entschlüsselungsinformationen für die jeweilige Magnetkarte extrahiert.

Ein Kopieren der Daten von Magnetkarten durch ein einfaches Lese-/Schreibgerät wird durch die erfindungsgemäß verschlüsselte Magnetkarte unmöglich. Die unterschiedliche Koerzitivität von Muster und Magnetstreifen und das auf nahezu jeder Magnetkarte verschiedene Muster führen dazu, daß die vom Magnetstreifen einer ersten Magnetkarten im Lesekopf induzierte Spannung nicht proportional dem Schreibstrom des Schreibkopfes für den Magnetstreifen einer zweiten Magnetkarte ist. Die von einer ersten Magnetkarte gelesenen Daten werden dadurch falsch auf eine zweite übertragen. Die Folge ist, daß die kopierte Magnetkarte völlig falsche Daten enthält oder ganz unlesbar ist.

Auch ein Kopieren der Magnetkarten durch mittiges Durchschneiden des Magnetstreifens in Längsrichtung wird durch die erfindungsgemäße Verschlüsselung der Daten verhindert. Das Aufbringen eines beliebigen Musters erlaubt es auch, Muster aufzubringen, die asymmetrisch relativ zur Längsachse des Magnetstreifens sind. Das hat zur Folge, daß man durch Längsteilung des Magnetstreifens zwei Magnetstreifen mit unterschiedlichen magnetischen Mustern erhält. Mit hoher Wahrscheinlichkeit sind die beiden halben Magnetstreifen mit den darauf enthaltenen Daten unlesbar. Dies kommt daher, daß die Daten ursprünglich mit den Entschlüsselungsinformationen, die aus dem gesamten Magnetstreifen ermittelt wurden, gespeichert wurden. Beim Einlesen eines halben Magnetstreifens werden sich nun aufgrund der unterschiedlichen Position und Ausdehnung des magnetischen Musters andere Entschlüsselungsinformationen ergeben, mit denen die ursprünglich auf der Magnetkarte abgelegten Daten nicht entschlüsselbar sind.

Eine bevorzugte Ausführungsform der Erfindung sieht vor, daß die Koerzitivität des magnetischen Materials des Musters ein Mehrfaches der Koerzitivität des Magnetstreifens aufweist.

Zwischen der Koerzitivität des magnetischen Materials des Musters und der Koerzitivität des Materials des Magnetstreifens besteht ein deutlicher Unterschied. Dadurch wird es ermöglicht, daß das Muster eindeutig von dem Magnetstreifen unterschieden werden kann. Möglicherweise bei der Lokalisation des magnetischen Musters auftretende Probleme aufgrund eines zu geringen Unterschiedes zwischen der Koerzitivität des Musters und der des Magnetstreifens werden so vermieden. Die Anzahl der unlesbaren oder fehlerhaft verschlüsselten Magnetkarten wird auf ein Minimum reduziert.

Weitere Ausführungsformen der Erfindung sehen vor, daß das beliebige Muster eine zufällige oder eine geordnete Form aufweist.

Das Muster wird durch unterschiedliche magnetische Materialien auf dem Magnetstreifen aufgebracht. Denkbar sind beispielsweise magnetische Dispersionen, magnetische Späne oder Folien aus magnetischen Materialien. Die Form des Musters kann dabei dem Zufall unterliegen oder aber geordnete Formen aufweisen. Solche geordneten Formen des magnetischen Musters sind beispielsweise geometrische Formen oder Buchstabenkombinationen.

Bei beiden Formen des magnetischen Musters muß allerdings darauf geachtet werden, daß der Magnetstreifen und das magnetische Muster eine einheitliche Farbe aufweisen, um zu verhindern, daß die Position und Ausdehnung des magnetischen Musters von außen optisch sichtbar ist und daraus die Informationen zur Entschlüsselung der Daten gewonnen werden können. Es ist jedoch denkbar, beispielsweise zu Werbezwecken, zusätzlich zum magnetischen Muster in der Farbe des Magnetstreifens ein weiteres farbiges Muster in Form eines Firmenlogos oder einer Buchstabenkombination in einer Farbe anzubringen, die sich von der Farbe des Magnetstreifens unterscheidet.

Im folgenden soll die Erfindung anhand einer Zeichnung und eines Flußdiagrammes näher erläutert werden. Es zeigen:

Fig. 1 eine Ausführungsform der erfindungsgemäß verschlüsselten Magnetkarte;

Fig. 2 ein Flußdiagramm zum Entschlüsseln und Wiederverschlüsseln der Daten auf einer erfindungsgemäß verschlüsselten Magnetkarte.

In **Fig.** 1 ist eine Magnetkarte mit der Bezugsziffer **1** gekennzeichnet. Auf einem Trägermaterial **2** ist ein Magnetstreifen **3** aufgebracht. Das Trägermaterial **2** besteht beispielsweise aus Papier oder Kunststoff. Zum Verschlüsseln der auf dem Magnetstreifen gespeicherten Daten wird dieser mit einem magnetischen Muster **4, 5** versehen. Das Muster **4, 5** besteht beispielsweise aus magnetischen Spänen, magnetischer Dispersion oder Folie aus magnetischen Materialien und wird auf dem Magnetstreifen **3** aufgebracht. Das magnetische Muster **4, 5** kann beliebige Formen haben. Das Muster **4** hat eine zufällige Form, wohingegen das Muster **5** eine geordnete Form, beispielsweise eine Buchstabenkombination, aufweist.

In **Fig.** 2 ist ein Flußdiagramm dargestellt, welches die verschiedenen Schritte beim Entschlüsseln und Verschlüsseln der Daten auf dem Magnetstreifen einer erfindungsgemäß verschlüsselten Magnetkarte näher erläutert. Als erstes werden die Position und die Ausdehnung des magnetischen Musters auf dem Magnetstreifen und die Koerzitivität des Magnetstreifens abhangig vom Flußwechsel ermittelt. Aus diesen Angaben werden die Entschlüsselungsinformationen extrahiert. Mit Hilfe dieser Entschlüsselungsinformationen werden aus den eingelesenen, verschlüsselten Daten die Rohdaten ermittelt. Diese Rohdaten werden dann aufgrund externer Ereignisse manipuliert; beispielsweise wird die Gültigkeitsdauer der Magnetkarte verlängert. Diese manipulierten Rohdaten müssen dann wieder auf die Karte geschrieben werden. Mit Hilfe der Entschlüsselungsinformationen werden die Rohdaten wieder verschlüsselt und durch entsprechendes Steuern des Schreibstromes eines Schreibkopfes auf dem Magnetstreifen der Magnetkarte abgespeichert.

Patentansprüche

1. Magnetisches Speichermedium, insbesondere eine Magnetkarte (1) mit einem Magnetstreifen (3), auf dem Rohdaten mit einem bestimmten Informa-

tionsgehalt in verschlüsselter Form abgespeichert sind, **dadurch gekennzeichnet**, daß auf dem Magnetstreifen (3) ein beliebiges Muster (4, 5) aus einem magnetischen Material mit einer von der Koerzitivität des Magnetstreifens (3) abweichenden Koerzitivität aufgebracht ist.

2. Magnetisches Speichermedium nach Anspruch 1, dadurch gekennzeichnet, daß die Koerzitivität des magnetischen Materials des Musters (4, 5) ein Mehrfaches der Koerzitivität des Magnetstreifens (3) aufweist.

3. Magnetisches Speichermedium nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß das beliebige Muster (4, 5) eine zufällige Form (4) aufweist.

4. Magnetisches Speichermedium nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß das beliebige Muster (4, 5) eine gezielte Form (5) aufweist.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 195 35 019 A1
Int. Cl.[6]: G 11 B 5/70
Offenlegungstag: 27. März 1997

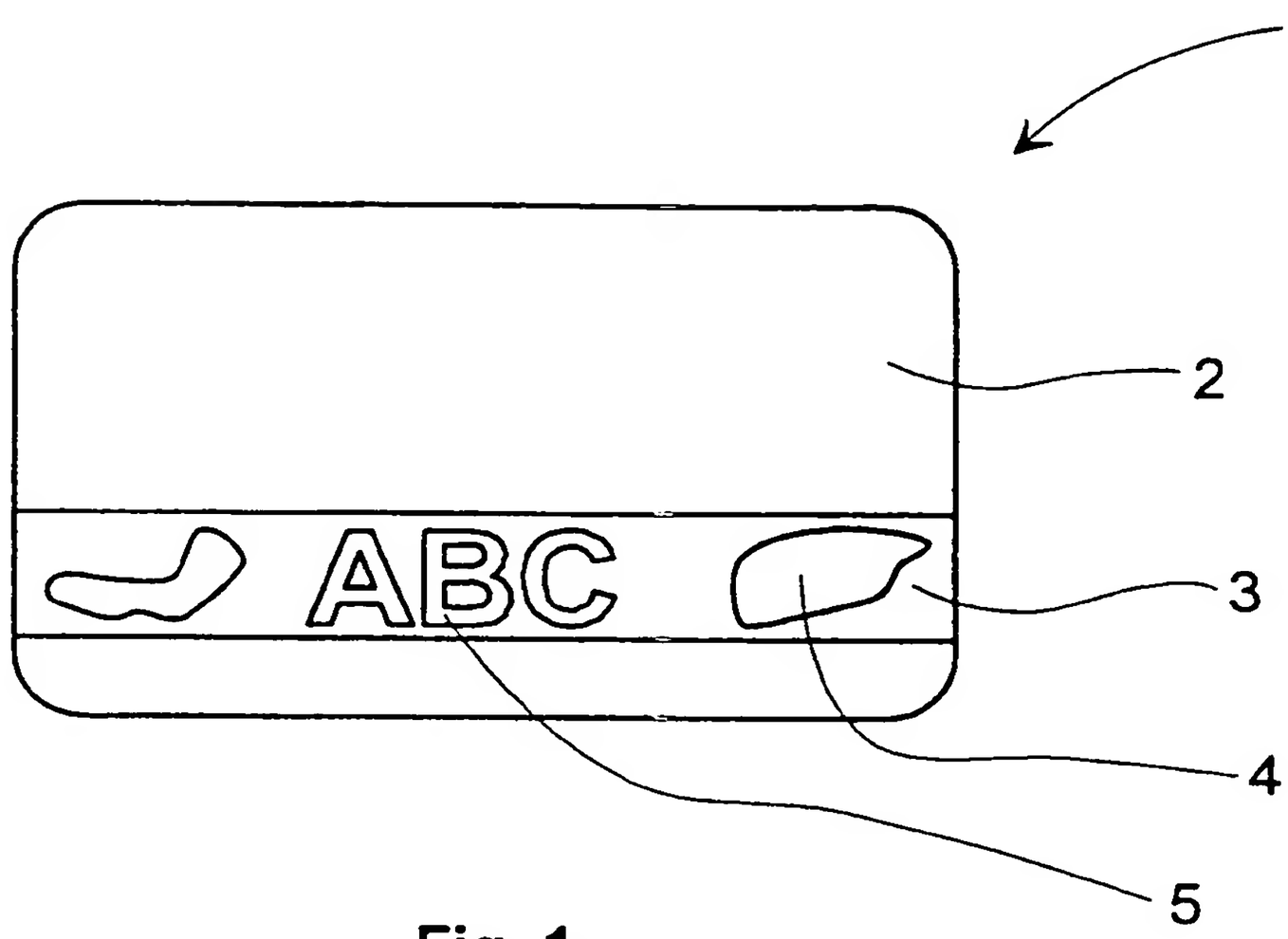


Fig. 1

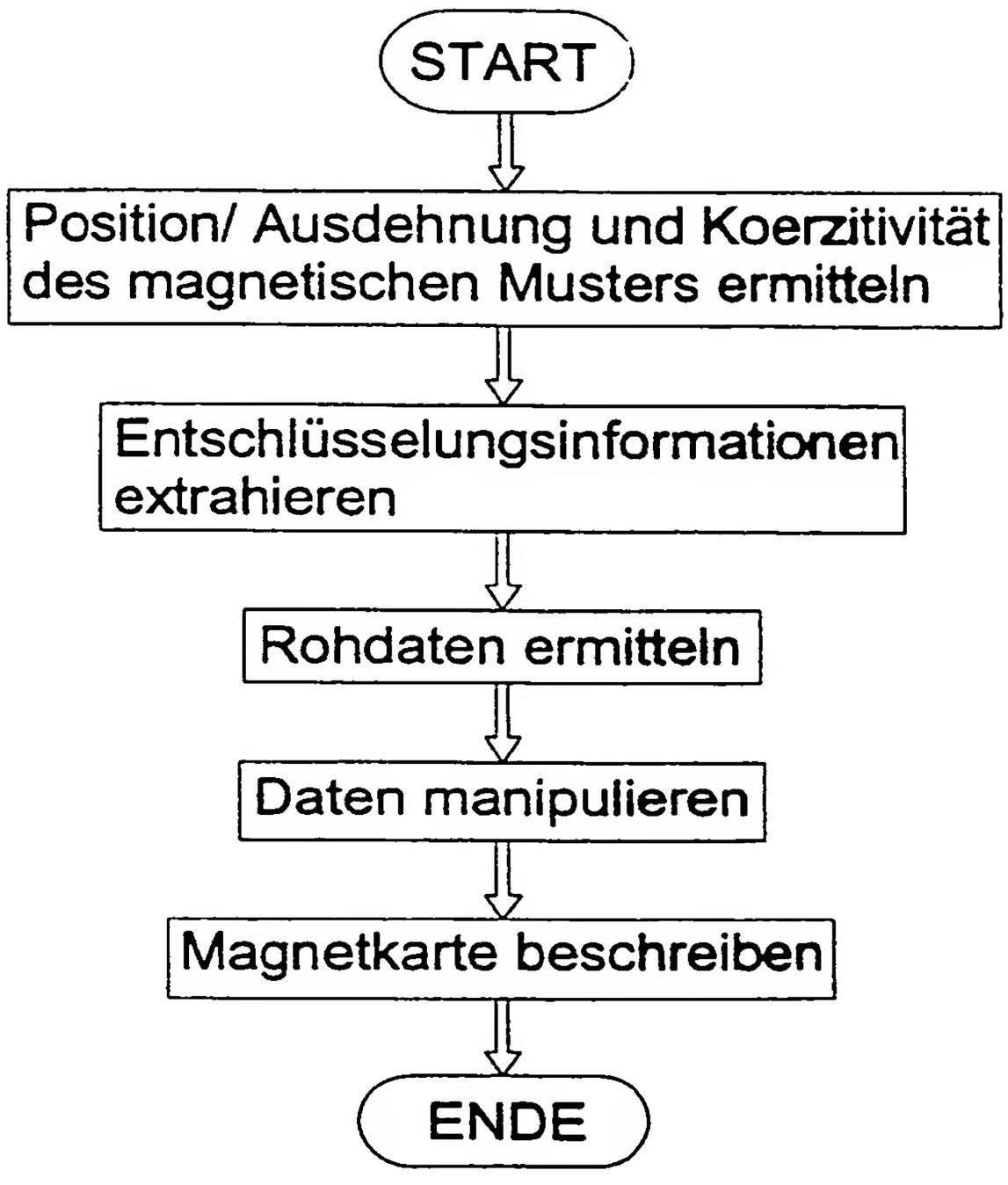


Fig. 2